Claims

What Is Claimed Is:

1. A method for providing user authentication comprising:

(a) sending, by a first unit, user identification data to an authentication unit;

(b) using the user identification data to determine which destination unit will receive an authentication code to be used to authenticate the user;

(c) sending the authentication code to the determined destination unit based on the user identification data;

(d) returning the authentication code to the authentication unit; and

(e) authenticating the user when the returned authentication code matches the sent authentication code.

2. The method of claim 1 including the step of generating the authentication code on a per authentication session basis and sending the authentication code to the determined destination unit in response to the generated authentication code.

3. The method of claim 1 including the step of maintaining per user destination unit data including at least one destination unit identifier per user [phone number, IP address] and wherein the step of using the user identification data to determine which destination unit will receive the authentication code includes sending the authentication code to the determined destination unit based on the stored per user destination unit identifier.

4. The method of claim 1 including the step of receiving user input in response to the step of sending the authentication code and waiting to return the authentication code to the authentication unit until receipt of the user input.

5. The method of claim 1 including the steps of:

prior to returning the authentication code to the authentication unit, digitally signing, by the first unit, the returned authentication code to produce a digitally signed authentication code that was received from the determined destination unit; and

verifying [by the authenticating unit,] the digitally signed authentication code as part of step (e).

6. A method for providing user authentication comprising:

receiving, from a first unit, user identification data by an authentication unit;

using the user identification data to determine which destination unit, other than the first unit, will receive an authentication code to be used to authenticate the user;

sending the authentication code to the determined destination unit based on the user identification data;

receiving a returned authentication code back after sending the authentication code; and

authenticating the user, based on the returned authentication code when the returned authentication code matches the sent authentication code.

7. The method of claim 6 including the step of generating the authentication code on a per authentication session basis and sending the authentication code to the determined destination unit in response to the generated authentication code.

8. The method of claim 6 including the step of maintaining per user destination unit data including at least one destination unit identifier per user and wherein the step of using the user identification data to determine which destination unit, other than the first unit, will receive the authentication code includes sending the authentication code to the determined destination unit based on the stored per user destination unit identifier.

9. The method of claim 6 wherein the returned authentication code is digitally signed and including the step of verifying, by the authenticating unit, the digitally signed authentication code as part of the step of authenticating the user, based on the returned authentication code when the returned authentication code matches the sent authentication code.

10. A method for providing user authentication comprising:

sending primary authentication information on a primary wireless channel by a primary authentication information provider to an authentication unit during a session;

using the primary authentication information to determine which destination unit will receive an authentication code as secondary authentication information via a wireless back channel to be used to authenticate the user;

sending the authentication code on the wireless back channel to the destination unit based on the primary authentication information during the same session;

returning the authentication code on the wireless primary channel to the authentication unit during the same session; and

authenticating the user when the returned authentication code received from the wireless primary channel matches the sent authentication code that was sent on the wireless back channel.

11. The method of claim 10 including the steps of generating and sending the authentication code on a per authentication session basis.

12. The method of claim 10 including the step of maintaining per user destination unit data including at least one destination unit identifier per user and wherein the step of using the primary authentication information to determine which destination unit will receive the authentication code includes sending the authentication code to the destination unit based on the stored per user destination unit identifier.

13. The method of claim 10 including the step of receiving user input in response to the step of sending the authentication code and waiting to return the authentication code to the authentication unit until receipt of the user input.

14. The method of claim 10 including the steps of:

prior to returning the authentication code to the authentication unit, digitally signing, by the first unit, the returned authentication code to produce a digitally signed authentication code that was received from the determined destination unit; and

verifying the digitally signed authentication code as part of authenticating the user.

15. The method of claim 10 including the step of sending the authentication code on the wireless back channel [or data based on it] to the destination unit using at least one of a short message session (SMS) channel, a paging channel and a control channel.

16. The method of claim 10 including the step of: validating the primary authentication information.

17. A storage medium comprising:

memory containing executable instructions that when executed by one or more processors, causes the one or more processors to:

receive, from a first unit, user identification data by an authentication unit;

use the user identification data to determine which destination unit, other than the first unit, will receive an authentication code to be used to authenticate the user;

send the authentication code to the determined destination unit based on the user identification data;

receive a returned authentication code back after sending the authentication code; and

authenticate the user, based on the returned authentication code when the returned authentication code matches the sent authentication code.

18. The storage medium of claim 17 including memory containing instructions that when executed by one or more processors, causes the one or more processors to generate the authentication code on a per authentication session basis and send the authentication code to the determined destination unit in response to the generated authentication code.

19. The storage medium of claim 17 including memory containing instructions that when executed by one or more processors, causes the one or more processors to maintain per user destination unit data including at least one destination unit identifier per user and send the authentication code to the determined destination unit based on the stored per user destination unit identifier.

20. The storage medium of claim 17 including memory containing instructions that when executed by one or more processors, causes the one or more processors to digitally sign the returned authentication code and verify, by the authenticating unit, the digitally signed authentication code as part of authenticating the user, based on the returned

authentication code when the returned authentication code matches the sent authentication code.

21. A storage medium comprising:

memory containing executable instructions that when executed by one or more processors associated with one or more devices, causes the one or more processors to:

send primary authentication information on a primary wireless channel by a primary authentication information provider to an authentication unit during a session;

use the primary authentication information to determine which destination unit will receive an authentication code as secondary authentication information via a wireless back channel to be used to authenticate the user;

send the authentication code on the wireless back channel to the destination unit based on the primary authentication information during the same session;

return the authentication code on the wireless primary channel to the authentication unit during the same session; and

authenticate the user when the returned authentication code received from the wireless primary channel matches the sent authentication code that was sent on the wireless back channel.

22. The storage medium of claim 21 containing memory having executable instructions that when executed by one or more processors, causes the one or more processors to generate and send the authentication code on a per authentication session basis.

23. The storage medium of claim 21 containing memory having executable instructions that when executed by one or more processors, causes the one or more processors to maintain per user destination unit data including at least one destination unit identifier per user and send the authentication code to the destination unit based on the stored per user destination unit identifier.

24. The storage medium of claim 21 containing memory having executable instructions that when executed by one or more processors, causes the one or more processors to receive user input in response to the step of sending the authentication code and wait to return the authentication code to the authentication unit until receipt of the user input.

25. The storage medium of claim 21 containing memory having executable instructions that when executed by one or more processors, causes the one or more processors to:

prior to returning the authentication code to the authentication unit, digitally signing, by the first unit, the returned authentication code to produce a digitally signed authentication code that was received from the determined destination unit; and

verifying the digitally signed authentication code as part of authenticating the user.

26. The storage medium of claim 21 containing memory having executable instructions that when executed by one or more processors, causes the one or more processors to send the authentication code on the wireless back channel to the destination unit using at least one of a short message session (SMS) channel, a paging channel and a control channel.

27. A system for providing user authentication comprising:

a first unit;

a second unit operatively coupleable to the first unit via a primary wireless channel and operatively coupleable to an authenticator; and

a third unit, operatively coupleable to the second unit via a wireless back channel,

the first unit operative to send primary authentication information via the primary channel during a session to the second unit;

the authenticator operative to use the primary authentication information to determine which destination unit, other than the first unit, will receive an authentication code as secondary authentication information via the wireless back channel and wherein the destination unit is the third unit;

the second unit operative to the send the authentication code on the wireless back channel to the destination unit based on the primary authentication information sent via the primary channel during the same session;

the first unit operative to return the authentication code on the wireless primary channel to the second unit during the same session; and

the authenticator operative to authenticate the user when the returned authentication code received from the wireless primary channel matches the sent authentication code that was sent on the wireless back channel.

28. The system of claim 27 wherein the authenticator maintains per user destination unit data including at least one destination unit identifier per user and sends the authentication code to the second unit for transmission to the destination unit based on the stored per user destination unit identifier.

29. The system of claim 27 wherein the first unit includes an interface to receive user input in response to the sending of the authentication code and wherein the first unit waits to return the authentication code for the authenticator until receipt of the user input.

30. The system of claim 27 wherein the first unit includes a cryptographic engine and prior to the first unit returning the authentication code for the authenticator, digital signs the returned authentication code to produce a digitally signed authentication code that was received from the third unit; and wherein the authenticator verifies the digitally signed authentication code as part of authenticating the user.

31. The system of claim 27 wherein the second unit send the authentication code on the wireless back channel to the third unit using at least one of: a short message session (SMS) channel, a paging channel and a control channel.